

Published and Copyright (c) 1999 - 2012
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

<http://people.delphiforums.com/dpj/a-one.htm>
Now available:
<http://www.atarinews.org>

Visit the Atari Advantage Forum on Delphi!
<http://forums.delphiforums.com/atari/>

==~==~==

~ Big Pay for HP's CEO! ~ Facebook's Good & Bad! ~ Man Dies Playing Games

- * East-West "Cold War" Is Risk *-
- * Super-Team of Veteran Atari Devs! *-
- * Anonymous Hacks An Anti-Hacking FBI Call! *-

==~==~==

->From the Editor's Keyboard

"Saying it like it is!"

Happy Groundhog Day!! I have no idea whether or not the furry animal saw his shadow or not, whether there will be 6 more weeks of winter or not. But, we're now in February and there's not a drop of snow on the ground in my neighborhood! While I'm a native New Englander, growing up in all kinds of winter experiences, I don't miss having to shovel tons of snow on a regular basis! And, after last year's winter, this is well-deserved reprieve!

So, ready for an Obama-Romney presidential election? It seems like this is going to be the choice that we'll face. I feel that Gingrich will end up self-destructing (thankfully), and the other candidates are already too far behind to be viable choices. This could be a scary election!

Until next time...

==~==~==

->In This Week's Gaming Section - Super-Team of Veteran Developers!
***** 100-Year-Old Plays Nintendo DS!
Taiwan Man Dies Playing Games!

==~==~==

->A-ONE's Game Console Industry News - The Latest Gaming News!

Atari Assemble! Super-Team of Veteran Developers Embrace Mobile Gaming

The good old 8-bit band is getting back together. Seamus Blackley, the co-creator of Microsoft's Xbox, has assembled a super team of Atari's original programmers to form a game studio meant to re-revolutionize the

gaming industry.

Blackley grabbed 11 of Atari's game creators to form Innovative Leisure, a gaming company focused on developing mobile titles. The "Jedi Council," as Blackley refers to the Atari developers, will include: Ed Rotberg (Battlezone), Owen Rubin (Major Havoc, Space Duel), Rich Adam (Gravitar, Missile Command), Ed Logg, (Asteroids Centipede), Dennis Koble (Touch Me, Shooting Gallery), Bruce Merrit, (Black Widow), and Tim Skelly, the only non-Atari developer. Innovative Leisure, though comprised of Atari veterans, is unassociated with Atari.

Blackley believes that Innovative Leisure can reignite that Atari magic and create a string of mobile gaming hits to rival (or at least compare) to Atari's original string of hits back in the '70s. Blackley has invested his own money with some help from game publisher THQ to support the Jedi Council and a team of young interns and turn their games into products.

The thing is, there aren't any official games on the schedule yet. Atari was able to create such amazing hits because of its collaborative, try-anything approach and the close-knit working relationships between its star developers. Blackley is bringing that spirit back by allowing his Atari vets to riff on game ideas, honing and refining their game prototypes until they come up with a hit. While its refreshing to see a studio committed to creating the best games possible, it also means there's little to show at the moment.

Atari largely defined the video game industry when it launched in the mid 1970s. The company was a huge hit in arcades but suffered a sharp decline after the collapse of the home-gaming market in 1983. Blackley and Innovative Leisure are hoping to right past wrongs and mobile - the very latest in personal gaming - is the ticket. He sees mobile as the new arcade, where gamers can buy simple games on the cheap and where quality - not marketing, glitz, or huge budgets -- will ultimately win the day.

100-Year-Old Grandmother Plays Nintendo DS Games To Keep Her Mind Active

Close your eyes, and try to imagine yourself beyond your 80th birthday. Do you still see yourself spending a couple of hours each day gaming? That's what 100-year-old Kathleen Connell does, and she says it's the reason why she doesn't "feel a day over 80."

The grandmother of one received her first Nintendo DS console from her daughter for her 96th birthday, and she's been hooked ever since. In fact, she's currently on her second one since she already wore out her first. She plays around two hours each day, drawing pictures or solving puzzles on any of the 10 games she keeps that includes Scrabble, Art Academy, and Brain Trainer.

When asked how gaming on the Nintendo DS has helped her, Kathleen told The Sun UK, "The Nintendo has been a great help to me, it's absolutely amazing. If there's any secret to a long life it's to think positive and keep your mind active."

A Taiwanese man died while playing video games at an Internet cafe as dozens of other patrons carried on for hours afterwards apparently unaware that they were sitting near a corpse, according to police.

The 23-year-old checked in at the cafe in New Taipei city on Tuesday night and was found dead but still sitting rigidly on a chair with his hands stretched out the following night by a waitress, police said.

The waitress last saw him talking on the phone around noon on Wednesday and his body had apparently been sitting there for up to nine hours without any of the 30 other people in the cafe noticing.

An initial police investigation found he might have died of a cardiac arrest triggered by low temperatures.

==~==~==

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Disagreements on Cyber Risk East-West "Cold War"

With worries growing over computer hacking, data theft and the risk of digital attacks destroying essential systems, western states and their allies are co-operating closer than ever on cyber security.

But as they do so, the gulf between them and China and Russia - blamed for many recent hacks and with a very different and much more authoritarian view over the future of the Internet - grows ever wider.

Last week, Chinese officials turned down invitations to a privately-run conference of military and civilian experts on cyber security in London, telling organizers Defense IQ they would not attend due to a "low tide" in relations with the U.S., particularly its military. A senior Russian official also pulled out at the last moment, citing a failure to obtain a UK Visa in time - although other attendees suspected that might simply have been an excuse.

Western officials talk down such snubs. But they admit progress towards international agreement on "norms of behavior" in cyberspace remains a distant dream.

"It is worrying," says John Bassett, a former senior official at British signals intelligence agency GCHQ and now senior fellow at London's Royal United Services Institute. "If anything, in the last year the differences have become more apparent and there seems to have been little success in tackling them. There is a risk it could end up damaging the wider relationship."

Russia and China, it seems, have little appetite to tackle data theft whilst the West has no intention of acquiescing to Russian and Chinese

demands for a more controlled Internet.

Jim Lewis, a former U.S. foreign service officer and now senior fellow at Washington DC think tank the Centre for Strategic and International Studies, participates in regular semi-official meetings with China on cyber.

"There are several things coming together here," he says.

"There is the political difference over the freedom and future of the Internet. Then that gets tied together with the theft of commercial property - which itself becomes part of the wider trade issues.."

Already, Western officials and academics involved in talks say discussions on cyber between East and West have become much more difficult and more complex than on any other issue.

"This is going to be a very gradual process," says Christopher Painter, the U.S. State Department lead official on cyber policy. "There are obviously some very different visions of the future of the Internet... On intellectual theft, I'm not going to single out China or Russia but it's obviously something we take very seriously."

A November London conference organized by British Foreign Secretary William Hague was supposed to kickstart progress towards global consensus. But if anything, it looks to have simply exacerbated the differences. A follow-up conference in Budapest later this year could be similar, some fear.

"The London conference did seem to show a "non-flexible" attitude from both the West and East," says Tony Dyhouse, a leading cyber security specialist for UK defense firm Quinetiq. "Dare we coin the term "Cyber Cold War?""

In public, U.S. and other Western officials almost always decline to detail where they believe the plethora of recent cyber attacks have come from.

In the last year, they have included attempts to break into computer systems at the U.S. State Department and British Foreign Office and other highly publicized attacks on Lockheed Martin, Google, the NASDAQ and the International Monetary Fund amongst others.

But privately and occasionally on the record, they frequently point the finger at Russia and China. Both angrily deny any involvement, saying they too are victims of hacking.

But many Western security specialists say the evidence against both nations - particularly China - has become increasingly compelling.

"China is currently engaged in a maximal industrial espionage effort that it justifies internally in terms of a catch up strategy (with the West)," says Thomas Barnett, chief analyst at political risk consultancy Wikistrat and a former strategist for the U.S. Navy. "The key question here is: can China assume the mantle of intellectual property rights respect fast enough to avoid triggering economic warfare of the West... If it can't, then this is likely to get ugly."

PricewaterhouseCoopers consultant Tim Hind, a former intelligence chief at British bank Barclays, has few doubts.

"I think government circles and organizations now... have very good attribution," he says. "The question is what you do diplomatically with that attribution... I think our government sees our economic and political mission with China as more important than addressing the cyber issue."

Some believe the most promising avenue of negotiation might be to link it to one of Beijing's primary worries - the buildup of U.S. military forces in Southeast Asia.

"There is a deal to be made here involving the U.S. ceasing its intelligence gathering, naval and air activity off China's coast," Nigel Inkster, a former deputy chief of Britain's Secret Intelligence Service (MI6) and now head of political risk and transnational threats at London's International Institute for Strategic Studies, said late last year.

But others suspect the scale of Chinese responsibility might be overstated.

"One thing is certain - the 'in thing' to do is blame China and hence it is likely that at least some of the actions blamed on China will not be of that origin," said another European cyber security expert, speaking on condition of anonymity. "They've become a 'no questions asked' scapegoat."

Because of the focus on China, some experts say the scale of hacking from Russian territory is often ignored.

That, some suggest, is how Moscow was able to marshal so many "patriotic hackers" to paralyze Estonia's Internet during a political face-off in 2007 as well as attacking Georgian websites during the 2008 war. More recently, such hackers have targeted dissident websites.

Perhaps even more serious than worries over hacking, however, is the vast philosophical gulf between East and West.

Last year, both Russia and China saw a rise in Internet-fuelled unrest that they blamed in part on the West. Beijing's censors increasingly struggled to control micro-blogging on their relatively tightly regulated Internet, whilst recent protests against Vladimir Putin are seen further fuelling Russian desire for control.

In the run-up to the London meeting, Moscow and Beijing released a suggested "code of conduct" for the global Internet that would give national governments much more control over the Internet within their borders.

But Western states swiftly shot down such suggestions. Despite British hopes the Chinese and Russians would not feel "ambushed" at the London summit, they would have found much to dislike there.

"The Chinese see the Internet as an American construct, designed to provide the U.S. with military and commercial advantage," said Lewis, adding that Beijing suspected the West of fostering dissent within its borders as well as building powerful cyber weaponry with which to attack.

With almost every nation dramatically ramping up its military spending on cyber security - including offensive "cyber warfare" capabilities to attack essential networks, turn off power grids and cause massive disruption - some fear more serious confrontation.

In a worst-case scenario, a single damaging cyber attack could spark a wider conventional war or even nuclear confrontation - with the risk a nation might wrongly blame a rival government for the actions of a single hacker and strike back. The 2009 Stuxnet computer worm attack on Iran's nuclear program that reprogrammed sensitive equipment to tear itself apart was seen by many as a sign of things to come.

As with any potential military conflict, experts have long said the key to avoiding accidental escalation is the creation of "confidence building measures" between all sides such as meetings, hotlines and shared discussions over threats.

Senior officers from the newly launched U.S. Cyber Command and other officials have massively ramped up links with other military and civilian cyber agencies across NATO and the Western world. That process with China and Russia is at a much earlier stage, officials say. Some believe more should be done.

"Even if you have long-running cyber arms control negotiations that never really went anywhere, that would give you the chance to get conversation and contacts going," says former GCHQ official Bassett.

For now, many believe the greatest risk is that paranoia sets in on both sides, further entrenching positions.

"We are very tempted by a "Cold War" way of thinking," says Lewis at the Centre for Strategic and International Studies. "The problem is that that can be very self-fulfilling."

Anonymous Hack An Anti-Hacking FBI Call; Takes Down The Boston PD

Whether you agree with the tactics of hacker group Anonymous or not, you have to admit they have a good sense of irony. Earlier today, the group hacked an FBI conference call about ... the threat posed by Anonymous.

News of the hack spread quickly via Twitter, and a recording of the call was posted on YouTube. The FBI has confirmed the authenticity of the recording in a statement, saying that they are "hunting those responsible."

The FBI attack is only the latest in the group's #FFF initiative to cause trouble for the government today. The hacker group has been promising via Twitter that "Friday will be a VERY interesting day of #Anonymous."

Earlier in the day, Anonymous took over the Boston police website in retaliation for what Anonymous calls police "brutality against Occupy Boston." The Occupy group was evicted from the Rose Fitzgerald Kennedy Greenway on December 10, though marches and protests continue.

Microsoft Slams Google User Data Policy in New Ads

Microsoft Corp. slammed search rival Google Inc. with full-page ads Wednesday, saying that recent changes at Google that allow it to internally merge the data it collects on user activity across services such as YouTube

and Gmail are meant to allow advertisers to better target customers.

Google has touted the overhaul it announced last week as a simplification of detailed but obtuse policies and a way to provide a better user experience.

Microsoft offered up its own Web-based alternatives, saying for instance that users of its free email service, Hotmail, don't have to worry about the content of their emails being used to help target ads.

The attack ads appeared in papers including USA Today, The Wall Street Journal and New York Times.

"Every data point Google collects and connects to you increases how valuable you are to an advertiser," Microsoft says in the ad.

In response, Google published a blog post in which it refuted what it called "myths" about its new privacy policy, saying, "Our privacy controls have not changed. Period."

The company does not dispute that it serves up ads based on words in private emails written by users of Gmail, but says such scanning is automated and is similar to how many email providers filter out spam. It has operated that way since Gmail's introduction in 2004.

Both companies offer several controls to prevent advertisers from tracking users' online activity.

Online expert Danny Sullivan, editor-in-chief of the website Search Engine Land, said that Google's privacy policy simplification has turned into a public relations "nightmare," but only because it again focused attention on the kind of data that Google has collected for years.

He said Microsoft is in no position to point fingers, since it also collects a lot of user data from its search engine, Bing, and will adjust search results based on information it finds in users' Facebook accounts if they are logged in.

"I think they're largely about the same," Sullivan said. "It would not be hard to go through and pick any major Internet company, talk about the kind of data they collect and start getting people paranoid."

Stop Right There: EU Halts Google's New Privacy Policy

Google's intrusive new privacy policy has raised quite a few eyebrows here in the United States, but it's making even more waves in the EU. There, a joint regulatory commission of all 27 European nations has called for the web search giant to halt the implementation of its new privacy rules slated to go into effect March 1, 2012.

Data privacy in Europe is monitored by The Article 29 Working Party, a collective of government privacy authorities from the EU member nations. In a letter to Google yesterday, the group wrote, "we call for a pause in the interests of ensuring that there can be no misunderstanding about Google's commitments to information rights of their users and EU citizens, until we have completed our analysis." While Google is not legally bound to comply with the Article 29 request, they have respected the group's

requests in the past.

The EU has been drafting new, more-stringent privacy rules over the past month. They require Google and other internet companies to ask for permission before they can save or sell your data. You can also request your data be permanently deleted.

Hacked Companies Still Not Telling Investors

At least a half-dozen major U.S. companies whose computers have been infiltrated by cyber criminals or international spies have not admitted to the incidents despite new guidance from securities regulators urging such disclosures.

Top U.S. cybersecurity officials believe corporate hacking is widespread, and the Securities and Exchange Commission issued a lengthy "guidance" document on October 13 outlining how and when publicly traded companies should report hacking incidents and cybersecurity risk.

But with one full quarter having elapsed since the SEC request, some major companies that are known to have had significant digital security breaches have said nothing about the incidents in their regulatory filings.

Defense contractor Lockheed Martin Corp, for example, said last May that it had fended off a "significant and tenacious" cyber attack on its networks. But Lockheed's most recent 10-Q quarterly filing, like its filing for the period that included the attack, does not even list hacking as a generic risk, let alone state that it has been targeted.

A Reuters review of more than 2,000 filings since the SEC guidance found some companies, including Internet infrastructure company VeriSign Inc and credit card and debit card transaction processor VeriFone Systems Inc, revealed significant new information about hacking incidents.

Yet the vast majority of companies addressing the issue only used new boilerplate language to describe a general risk. Some hacking victims did not even do that.

"It's completely confusing to me why companies aren't reporting cyber risks" if only to avoid SEC enforcement or private lawsuits, said Jacob Olcott, former counsel for the Senate Commerce committee. The chair of that committee, John D. Rockefeller, urged the SEC to act last year.

Stewart Baker, a corporate attorney and former assistant secretary of the Department of Homeland Security, said the SEC guidance was detailed enough that companies that know they have been hacked will "have to work pretty hard not to disclose something about the scope and risk of the intrusion."

Otherwise, "this is an opportunity for enforcement that practically hands the case to the SEC on a platter," Baker said.

Lockheed spokesman Chris Williams said hacking was covered under the company's most recent annual securities filing, which has as one of many risk factors "security threats, including threats to our information technology infrastructure, attempts to gain access to our proprietary or classified information, threats to physical security of our facilities

and employees, and terrorist acts."

Williams said the May attack had "no material effect on our business."

Mantech International Corp, CACI International Inc and other defense and technology firms that have been reported by security researchers as hacking victims were likewise silent in their most recent filings. Neither Mantech nor CACI responded to interview requests.

"It's common knowledge" that most large defense contractors have been penetrated, said Olcott.

Sikorsky Aircraft, mindful of a strict New Hampshire law warning individuals at risk of identity theft, wrote to that state's attorney general in August that hackers had gotten into its system and could have accessed Social Security numbers of 55 employees who lived in the state.

Sikorsky said the employee data likely was not the hackers' target, which suggests that they might have been after designs or other trade secrets. But Sikorsky parent United Technologies Corp did not mention the May intrusion in subsequent SEC filings.

"Like other companies, our businesses are subject to (information technology) security attacks at times. We monitor systems and cooperate closely with the government when appropriate," said United Technologies spokesman John Moran.

Melissa Hathaway, a former intelligence official who led U.S. President Barack Obama's initial cybersecurity policy review and helped push the SEC to enact a disclosure policy, said she was "surprised" at the dearth of new confessions.

"The SEC division of corporate finance has an obligation to ask these companies why they didn't disclose," she said. "We need to have transparency on the state of the situation, and we need to have a national conversation regarding the near-term impact of economic espionage and the long-term health of the nation."

The SEC declined to comment. The agency's guidance officially clarifies previous policy instead of establishing a new rule, a process that takes longer and requires a vote of the commissioners. A person close to the agency said it expects fuller disclosures in annual 10-K filings that will begin appearing in volume this month.

Cybersecurity has been an increasing concern in Washington, and Obama asked during his State of the Union speech for action on legislative proposals. Security experts believe hackers are frequently targeting valuable digital information including strategic plans, blueprints and secret formulas.

But security experts in and out of government have complained for years that most companies don't disclose even very successful hacking attacks, because they never find out about them or simply don't want to spook investors, customers or business partners.

The U.S. National Counterintelligence Executive, in a landmark November report that openly accused China of sponsoring military and economic cyber espionage, said that it is hard for companies to estimate the impact of losses that might not be apparent for years.

One Pentagon contractor that did go into some detail recently about the threat was Northrop Grumman Corp, which warned: "Cybersecurity attacks in particular are evolving and include, but are not limited to, malicious software, attempts to gain unauthorized access to data, and other electronic security breaches that could lead to disruptions in mission critical systems, unauthorized release of confidential or otherwise protected information and corruption of data. These events could damage our reputation and lead to financial losses from remedial actions, loss of business or potential liability."

A few technology companies gave even more specific warnings, including Juniper Networks Inc, which makes gear for routing Internet traffic, and chip-maker Intel Corp. Intel had been one of the few to disclose a successful breach in the past, along with Google Inc, which has complained of attacks originating in China.

In a November filing, Intel repeated that hackers had gotten inside and warned that "the theft or unauthorized use or publication of our trade secrets and other confidential business information as a result of such an incident could adversely affect our competitive position and reduce marketplace acceptance of our products."

Some companies asserted that they had not been hacked, or at least averred that they had not been subject to a "material" or "catastrophic" intrusion.

Others confessed to breaches for the first time, including VeriSign and VeriFone Systems, which said it had experienced "security breaches or fraudulent activities related to unauthorized access to sensitive customer information."

The company did not respond to requests for elaboration. Point-of-sale terminals including VeriFone's models are popular targets for criminal hackers, who can tamper with them in order to record passwords and card numbers.

VeriFone has been reported as a supplier of machines to Michaels Stores Inc, a retail chain of hobbyist stores that had to replace more than 7,000 terminals last year after discovering tampering in 20 states.

Two other companies said they disclosed breaches because of the SEC guidance. Tumi Holdings, the luggage maker that is pursuing an initial public offering, said in a stock prospectus that security systems in some of its retail stores had been compromised in the past.

In an interview, Tumi Chief Financial Officer Michael Mardy said there had been no theft of a database or other massive breach. Instead, he said there had been occasions where store employees had conspired with outsiders on a small scale, for example by giving refunds to people who had not made purchases.

"We felt it was necessary to list as a risk factor because it actually is a risk factor," Mardy said.

University of Phoenix parent Apollo Group Inc, which in the past had noted attempted breaches, for the first time said some attempts had succeeded.

"We are facing an increasing number of threats to our computer systems of unauthorized access, computer hackers, computer viruses, malicious code, organized cyber attacks and other system disruptions and security

breaches, and from time to time we experience such disruptions and breaches," it wrote in a 10-Q.

Apollo spokesman Rick Castellano declined to say how extensive the breaches had been. "Cybersecurity is an area of growing area of concern for all companies", Castellano said. "We devote significant resources to manage any potential threat."

A Sobering Look at Facebook

It's the year's hottest initial public offering, but some wealth managers find themselves having a hard time recommending Facebook to their clients.

The world's biggest social network is expected to seek a \$75 billion to \$100 billion valuation in its IPO, the most anticipated stock offering from Silicon Valley since Google Inc went public in 2004.

At Granite Investment Advisors in New Hampshire, Chief Investment Officer Scott Schermerhorn has already been fielding queries from clients eager to get in on the action.

"We had some clients call and once we step them through the numbers, they sober up," he said. "The valuation is 100 times earnings in a stock market that is trading at 12."

"At the end of the day, if you have a small amount of money that you are in a position to lose a chunk of it and you want to speculate on Facebook, go ahead," he added. "But don't use money that you really need to save to do it. I would put it in Microsoft, which is dirt cheap right now."

To be sure, most technology analysts would argue that Facebook's growth potential far exceeds that of Microsoft Corp, whose stock has largely traded between \$20 and \$30 in the past decade. It is taking its first steps toward content streaming for instance, and has yet to make a serious overseas thrust.

And a \$100 billion valuation for Facebook at the top end - while huge in absolute terms - is not that out of whack in Silicon Valley IPO tradition. Facebook is seeking a multiple of up to 27 times annual revenue, or up to 100 times earnings.

Apple Inc - today, the world's most valuable technology corporation - went public at a valuation of just \$1.19 billion in 1980, equivalent to 25 times revenue and 102 times earnings. Google - to which Facebook is most often measured against in terms of potential - was valued at \$23 billion at the time of its 2004 debut, or 218 times earnings.

But the sheer size of Facebook's valuation means that it will have to become the world's first \$700 billion company if it is to replicate the gain in Google's stock.

"At these valuations, investors really need to set aside emotion...and invest with their heads," said Edward Reinhart, managing partner at Capital Advisors Wealth Management, who owns Facebook shares bought on private markets two years ago.

Reinhart, who advises clients on retirement planning, warned that hype

building up ahead of Facebook's IPO could mean "dangerous waters for the retail investor."

Facebook, led by 27-year-old Mark Zuckerberg, on Wednesday filed its IPO prospectus with the Securities and Exchange Commission, seeking to raise \$5 billion.

The anticipation surrounding the company and its growth potential recalls the hoopla that accompanied Apple's, Google's, and Amazon.com Inc's stock debuts. All three companies have done the near-impossible - lived up to the hype.

There are many who believe Facebook will do the same, pointing to its 843 million users and the fact that the company is much bigger and more profitable than other recent Internet debuts, such as the loss-making Pandora Media Inc or Groupon Inc.

Social game company Zynga closed up nearly 17 percent on Thursday in the first trading session after Facebook revealed it made 12 percent of its revenue last year from the video game publisher.

"Facebook has the most potential," said Greenwich, Connecticut-based investment manager Jeff Matthews, speaking about its business plan rather than its stock price. "It's the next Google."

While retail investors are still combing through the numbers and doing the math, institutional investors have quietly bought Facebook shares via private pre-IPO exchanges like SharesPost and SecondMarket.

About 50 equity funds of the 3,842 tracked by Morningstar disclosed holdings of Facebook stock, led by Morgan Stanley's institutional Opportunity H fund with 3.5 percent of its \$242 million portfolio devoted to the social network.

Other funds that have disclosed holdings included those managed by Fidelity, T. Rowe Price, ING, Principal and MassMutual.

As with Apple and Google, consumers feel strong emotional connections to Facebook, which could make its stock vulnerable to wild swings if it attracts many retail investors.

When the SEC released Facebook's IPO prospectus on Wednesday evening, its website slowed to a crawl as traffic increased 100 times. Facebook also made it into betting books - Irish bookmaker Paddy Power is taking bets on what the share price will be when the social network begins trading.

The odds are 7 to 2 so far that investors will be paying between \$25 and \$34.99 for a share, according to the bookmaker.

"The challenge is trying to keep individual investor enthusiasm in some sort of line with economic reality," said Lise Buyer, an IPO adviser who worked at Google at the time of its IPO, but hasn't worked on the Facebook IPO.

Facebook "has very strong prospects, but all companies have stock prices that at some point must correlate to fundamentals."

The social network's 2011 revenue rose 88 percent to \$3.71 billion while net profit increased 65 percent to \$1 billion in last year. Those are not stellar numbers when compared with Apple's 65 percent growth in revenue to

\$108.24 billion in fiscal 2011. Apple also outpaced Facebook in terms of income growth, with profit increasing 85 percent to \$25.92 billion.

Despite this, Apple - with nearly \$100 billion in cash and securities - trades at a forward price-to-earnings ratio of 13 times, far lower than the 100 times historic P/E of Facebook's IPO, assuming the \$100 billion valuation.

Even Microsoft - which saw net income grow 23 percent to \$23.1 billion and revenue rise 12 percent to 69.9 billion for fiscal 2011 - trades at 11 times future earnings.

That's why Schermerhorn, whose firm already owns Apple shares, said he preferred to invest in Microsoft over Facebook. Amazon's shares trade at a relatively dear forward P/E of 131, while Google trades at 19.5.

"I know it is dominant in its space. Granted, the space is not growing as quickly as Facebook, but I am getting a nice dividend to wait," he said of Microsoft. "I don't have that with Facebook."

Symantec Says pcAnywhere Safe, Offers Free Upgrade

Symantec Corp said it is safe to use its pcAnywhere software for accessing remote PCs after it asked customers last week to disable the product because it put them at greater risk of being hacked.

The software maker took the unusual step of urging customers to temporarily stop using the product after an investigation determined that the blueprints, or source code, to pcAnywhere were stolen in 2006.

Symantec said on January 25 that the theft put users of all versions of the product at greater risk of losing data to hackers.

The company has since determined that it was safe to use the current version of the product, pcAnywhere 12.5, as long as it was updated with a security patch released on January 23, company spokesman Brian Modena said on Monday.

Symantec is offering free upgrades to pcAnywhere 12.5 at no charge to all customers, even those using old editions that would not typically qualify for support, he said.

The company warned customers earlier this month about the theft of the source code to pcAnywhere and several other titles such as Norton Antivirus Corporate Edition, Norton Internet Security, Norton Utilities and Norton GoBack.

It made the announcement after a hacker who goes by the name YamaTough released the source code to its Norton Utilities PC software and threatened to publish its widely used anti-virus programs. Authorities have yet to apprehend the hacker.

The company initially said the theft of the code posed no threat as long as customers were using the most recent versions of Symantec's software, with one exception - users of pcAnywhere might face "a slightly increased security risk."

While Symantec is advising all customers to upgrade, they can safely continue using versions 12.0 and 12.1 if they download a second software patch released on January 27, Modena said.

Customers can contact the company via email for more information: pcanywhere@symantec.com.

Internet Explorer 9 Growing Fast on Windows 7 PCs

Windows users can't get enough of Internet Explorer 9. That's the message Microsoft is driving hard, releasing statistics that show its most recent web browser is growing strong among users of Windows 7 PCs.

IE9 is now the primary browser on 36.2% of Windows 7 machines, Microsoft revealed in a blog post based on statistics from Net Applications, up 2% since December. It passed IE8 back in November and has been ticking up ever since as more people make the switch to Windows 7 (IE8 is the last browser compatible with Windows XP).

Microsoft attributes the rapid growth to consumer desire for a "modern browser" experience, complete with compatibility with HTML5 apps. As an example, it cited the game Cut the Rope, which Microsoft brought to the web in January via a partnership with the makers of the game. However, there are plenty of modern browsers, as Microsoft defines them, so there must be other factors at work, and one of them is surely the fact that IE9 is the default browser on any new Windows PC.

Microsoft fully released IE9 to the public on March 14. Although it added many features to make it more competitive with other browsers such as Firefox, developers have had a shaky relationship with the browser. Since IE9's market share is so large, web designers must make sites compatible with it, but some have expressed disappointment with some of its workings.

While IE9 may rule the world of Windows 7, Google Chrome is the current king of the browser heap. Chrome 15 is the most popular browser in the world, according to StatCounter, recently passing IE8.

Microsoft is currently testing the next version of its browser, Internet Explorer 10. IE10 will be the first version of the browser to be fully compatible with the upcoming Windows 8.

Facebook Will Never Charge You... Because It Already Does

The persistent rumor that Facebook will someday charge its users to access the site simply will not die. Since Facebook's early days, users have clamored around the myth that someday the social network would take captive their years' worth of photos, comments, friendships, and check-ins. And time after time, the myth has been busted.

Now the announcement of Facebook's IPO process has resurrected old fears, and yet again the rumors about a paid-for service are insufferably making the rounds. It's time to extinguish this thing once and for awhile, and this time we have new insight from the company S-1 to lend a little support. Facebook says it won't

This past fall yet another pay-for-Facebook induced craze hit the site as a result of the Timeline announcement. An alleged price grid announcing that there would be different subscription rates to use the site had users in a frenzy - enough so that Facebook actually commented on the rumors. On Facebook's official profile, the site cleared things up:

"A rumor on the Internet caught our attention. We have no plans to charge for Facebook. It's free and always will be."

And this coincides with the message on the login page.

Sure, things change when a company goes public, but this is completely central to Facebook's core. It simply makes no sense, unless you think Mark Zuckerberg and company originally set out to lure in users, trap their data, and make off with it like bandits while simultaneously tricking them into paying for a service they'd been duped by.

While we don't think Facebook is out to reel users into paying, we understand the cynicism when it comes to the site's intentions. This sort of tension between the site and its users over data-harboring has left some feeling exploited. Of course, both parties are to blame, and this system has to become an accepted necessary evil of using Facebook.

That said, read the S-1 and you might feel a little better. This excerpt particularly speaks to that, and it might help calm any fears:

"Our culture emphasizes rapid innovation and prioritizes user engagement over short-term financial results. Simply put: we don't build services to make money; we make money to build better services."

Time and time again Facebook insists it is focused on the user and that this sentiment will remain regardless of who owns what shares. In fact Facebook points out that even though it's currently not making them any money, it's been heavily investing in developing the mobile experience for users. It's sacrificed in other ways to keep users happy as well:

"From time to time, we have taken actions to reduce the volume of communications from apps to users on Facebook with the objectives of enhancing the user experience, and such actions have reduced distribution from, user engagement with, and our monetization opportunities from apps on Facebook."

Facebook isn't faultless, however, and if the site has stretched your patience and tried your trust one too many times, there's a much more calculated reason it won't charge you: it doesn't need to.

Facebook doesn't need your money because it's got something way more valuable - your data. Why would the site risk the ire of its users who are providing it content that it then turns into ad revenue? One of the risk factors Facebook identified is that it's facing increasing competition, and paid subscriptions would ward off new users and drive them elsewhere. From a business perspective, Facebook has everything it needs in your data.

The company's profits have been unstoppable since it launched, and its net gain grew 88-percent year over year between 2010 and 2011. It's got a good thing going, and just because it will bring new shareholders (who will still be minority shareholders) on board doesn't mean it's going to mess with success.

What users need to realize is that we do pay. Every time we use an app or click an ad, or even just hit the Like button or fill out our profile information, we re paying Facebook.

HP Awards New CEO Whitman with \$16.5 Million Pay Package

Hewlett-Packard Co. ushered in Meg Whitman as its CEO with a \$16.5 million compensation package. It hinges on whether the former candidate for California governor can lift the stumbling technology company's stock price during the next two years.

Last year's pay consists almost entirely of 1.9 million stock options valued at \$16.1 million. HP disclosed that amount for the first time in a Friday regulatory filing. The company announced Whitman would be getting the stock options shortly after her hiring, but didn't specify their value at that time.

Whitman is getting a \$1 salary while she tries to rebuild the momentum that HP lost after ousting Mark Hurd as its CEO in a titillating scandal in 2010.

Whitman replaced Hurd's successor, Leo Apotheker, last September.

Facebook's Popularity Also Brings Lawsuits

As Facebook readies for Wall Street's richest high-tech debut, it is wrangling with litigation and bracing for potential new suits.

The social network filed Wednesday for a \$5 billion stock offering that could create one of America's largest publicly traded companies.

But even as Facebook reinvents the way people around the world communicate, it anticipates a mountain of legal challenges which will take armies of lawyers years to disentangle.

In its filing with the Securities and Exchange Commission, Facebook hinted at some of the legal tangles ahead, writing that it is already embroiled in litigation and anticipates "numerous" more lawsuits in coming years.

"We are currently, and expect to be in the future, party to patent lawsuits and other intellectual property rights claims that are expensive and time-consuming, and, if resolved adversely, could have a significant impact on our business, financial condition, or results of operations," Facebook said.

Legal experts said there is virtually no corner of public life where Facebook's impact is not felt.

"Social media drastically affects almost every aspect of how society communicates," said Brian Wassom, a partner at Honigman Miller Schwarz and Cohn law firm in Detroit.

Wassom said the numerous types of possible legal challenges reflect the

unprecedented reach that Facebook has achieved in its few years of existence.

The company says it has over 845 million users including nearly half a billion who log in daily.

Ryan Calo, director for privacy at Stanford University's Center for Internet and Society, said the social network is "a real transformative communication platform."

"For better or for worse, this pattern is really accelerating," Calo said, speaking about Facebook's expanding reach.

Legal experts said the untold number of unresolved legal issues for users of Facebook, Twitter, Foursquare and other social networking sites cover every aspect of financial and personal transactions carried out between individuals.

For instance, can a prosecutor use elements gleaned from Facebook in making a legal case against a defendant? Is it possible to use Facebook to establish whether a loan applicant is a good credit risk?

Can law enforcement officials prosecute threats or intimidating statements posted on Facebook? How and when can an employer use information gathered on Facebook to discipline or terminate an employee?

Calo said the ubiquity of Facebook increases the urgency to update the legal roadmap governing how it can be accessed, and by whom.

"Facebook has become almost as indispensable as the telephone or radio," he said. "We need to make changes in laws or update our laws to reflect a new reality."

Pedram Tabibi, an attorney at the New York firm Melzer Lippe, said three businesses in four use some form of social media.

"The dependence on Facebook in people's personal lives is high, (and) the dependence on Facebook in business is increasing," Tabibi said, alluding to what he called the "intersection of two roads."

But slightly less than half of US companies have put in place ground rules on how their workers are to proceed in using social networking sites, Tabibi said, adding that firms that tarry are leaving themselves open to headaches.

Equally opaque are the conditions under which the US government can access the information on an individual's Facebook account, legal experts said.

Nebulous rules have not stopped the government however from deporting migrants or conducting broader investigations based on tips gleaned from Facebook.

"People now put their lives on Facebook," said Tabibi, adding that they need to exercise caution because that information "might be used against them."

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.